

REMARKS

Claims 4 to 6 are now pending in the present application. Applicant respectfully requests reconsideration of the present application in view of this response.

35 U.S.C. § 101

Claims 4 to 6 were rejected under 35 U.S.C. § 101 for purportedly lacking practical application in the technological arts. Applicant respectfully requests reconsideration of claim 4 to 6 and submits that those claims are statutory patentable subject matter. According to guidelines published by the USPTO, if the invention produces a useful result, i.e., the invention has a practical application in the technological arts, then it should not be rejected under 35 U.S.C. § 101.

Claims 4 to 6 concern a process for establishing a common cryptographic key for n subscribers using the Diffie-Hellman process. As explained in the Specification, this process has a practical application in the technological arts in that it provides a process to guarantee the secrecy of messages which are to be transmitted exclusively to a number of subscribers via insecure communication channels. See, e.g., page 1, lines 5-10. The present invention also provides a process wherein a group key is established with the aid of a tree structure in such a manner so that even after the group key has been established, subscribers can be removed from or added to the key directory without great effort. Accordingly, claims 4 to 6 do recite statutory patentable subject matter and withdrawal of the rejection under 35 U.S.C. § 101 of claims 4 to 6 is respectfully requested.

35 U.S.C. § 102(e) – Caronni reference

Claims 4 and 5 were rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,049,878 to Caronni et al. (“Caronni reference”).

The Caronni reference purportedly concerns a system for secure multicast including at least one sending entity operating on a sending computer system a number of receiving entities running on a receiving computer system, a traffic distribution component coupled to the sending entity and each of the receiving entities, and a participant key management component operating within each receiver entity. The Caronni reference recites that the participant key management component holds a first key that is shared with the sender and all of the receiving entities, and a second key that is shared with the sender and at least one but less than all of the receiving entities. The Caronni reference further recites that the group key management component is coupled to the traffic distribution component and includes a data structure for storing all of the participant first and second keys. At the passage of col. 2, lines

59-67, cited in the Office Action, the Caronni reference merely recites the use of certified Diffie-Hellman keys with the SKIP. SKIP is a public key certificate based key management scheme which provides group key management for internet protocols. At the passage of col. 6, lines 20 to 65, the Caronni reference recites that the participants 101 are identified with an ID number, and the bit pattern of the ID of each participant 101 defines which keys it shares with the group key manager. The Caronni reference recites that this may be represented as a binary tree with the manager 108 above the root being the traffic encryption key and the other shared secrets being among selected recipients 101 forming the leaves; and, further up, every node is populated by shared secrets known to more and more participants. The Caronni reference states that associated with each key is a version number and a revision number, used in the actual communication to notify the participants of key updates.

In contrast, claim 4 of the present invention is directed to a process for establishing a common cryptographic key for n subscribers using the Diffie-Hellman process, and requires at least the feature of *establishing secrets consecutively in a direction of the root of the tree for all k nodes of the tree starting from the n leaves of the tree across an entire hierarchy of the tree*, wherein *two already known secrets are combined using the Diffie-Hellman process to form a new common secret, the new common secret being allocated to a common node so that a common cryptographic key for all n subscribers is allocated to a last one of tree nodes, the last one of the tree nodes being the root of the tree*. The Caronni reference does not appear to identically describe this feature.

And, to anticipate under 35 U.S.C. § 102, the Patent Office must demonstrate that *each and every claim feature is identically described or contained in a single prior art reference*. See *Scripps Clinic & Research Foundation v. Genentech, Inc.*, 18 U.S.P.Q.2d 1001, 1010 (Fed. Cir. 1991). The Caronni reference does not identically describe each and every claim feature of claim 4 or its dependent claim 5.

Accordingly, Applicant respectfully submits that claim 4 is allowable; and respectfully requests withdrawal of the rejection of claim 4 and its dependent claim 5 under 35 U.S.C. § 102(e) over the Caronni reference.

In summary, it is respectfully submitted that all of claims 4 to 6 of the present application are allowable for the foregoing reasons.

CONCLUSION

In view of all of the above, it is believed that rejections under 35 U.S.C. §§ 101, 102(e), of the claims have been overcome. Accordingly, it is respectfully submitted that all claims 4 to 6 are allowable. It is therefore respectfully requested that the rejections be reconsidered and withdrawn, and that the present application issue as early as possible.

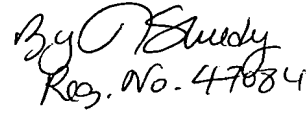
If it would further allowance of the present application, the Examiner is invited to contact the undersigned at the contact information given below.

Respectfully submitted,

Dated: November 17, 2005

By:




Reg. No. 47084

Richard L. Mayer (Reg. No. 22,490)

KENYON & KENYON

One Broadway

New York, New York 10004

(212) 425-7200 (telephone)

(212) 425-5288 (facsimile)

CUSTOMER NO. 26646